REMARKS

By the above amendment, applicants have amended claims to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention patentable over the prior art. In addition, applicants thank the Examiner for the clear and understandable Office Action.

The Rejection of Claims 1, 6, 8-11, 14, 15, 18, 19 and 20 Under 35 USC 103 (a) Overcome

The last O.A. rejected Claims 1, 6, 8-11, 14,15, 18, 19 and 20 for being unpatentable over Yu et al (US Patent No. 6,067,621), Vaeth et al (US Patent No. 6,035,402), and Brown et al (US Patent No. 6,658,415, M. Brown).

Claim 1

Claim 1 has been amended to clarify the novel feature of the "authentication authority web service" over the combination of referenced prior-art. Applicants request reconsideration of this rejection for the following reasons:

1) As explained in the following, the method and system described in Claim 1 solves a different problem and produces unexpected results. In addition, the prior-art references produce an inoperative combination or combination which does not meet Claim 1.

   The last O.A. notes (p. 5) that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Vaeth and M. Brown into the teaching of Yu to utilize a CA (i.e. gateway authority) to delegate authority to a RA (i.e. authentication authority) and to use the authentication handler for serving as a doorkeeper to protect the resource.

From Vaeth's (col. 6 lines 12-14) teaching for the function of a RA, i.e., **"(2) the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;",**

and from Vaeth's (col. 6 lines 14-19) teaching for the function of a CA, i.e., **"(3) the CA (a) generating the certificate with the requester's public key and the public key of the certificate authority, (b) signing the certificate using the private key of the certificate authority; and (c) delivering the certificate to the requester on the network.",**

it is recognized that the main function of the CA and RA is to process certificate requests, verify a requester's identities, generate/issue certificates, and lastly distribute certificates. Thus, the function of a CA and RA is vastly different from that of the authentication authority and gateway authority as defined by Claim 1. Vaeth does not suggest that we can utilize the CA and RA to authenticate a user's identity during the Internet online business transaction. In contrast, the method and system described in Claim 1 explain means to deliver authentication authority Web services using non-reusable and non-reversible one-time identity codes (or one-time passwords) over the Internet. Thus, applicants' invention solves a different problem than the referenced Vaeth's invention.

Furthermore, there is also a difference in defining the authority delegation process. According to the above mentioned Vaeth's teaching, the CA delegates the authority to the RA for processing certificate requests. The CA remains the sole authority to generate and sign new certificates. The main reason to have a RA for processing certificate requests is mainly for a security reason, i.e., from Vaeth's (col. 6 lines 49-57) teaching:

"An advantage of the present invention is that the CA may generate and host an Internet (or Intranet) web site on behalf of multiple RAs or have certificate requests to an RA-maintained web site linked invisibly to the CA to provide a "virtual CA". The network linking provides flexibility as to different applications and RA requirements. The distributed functionality minimizes RA investment and allows the CA to concentrate on providing security at the most security-sensitive portion of the system."

In contrast, the role of the gateway authority in Claim 1 is to "forward" the authentication request to the authentication authority as a part of the user authenticating process. The purpose of having the gateway authority is to achieve the scalable and distributable functionality for authenticating a user globally. Thus, it is obvious that the function of Vaeth's CA is very different from that of the gateway authority described in Claim 1.

As a result, the combination of Vaeth's teaching will produce a system that is inoperative for authenticating a user with one-time identity codes as described in Claim 1. To produce a workable system, a significant modification of Vaeth's teaching is necessary.

The last O.A. also notes (p.6) that M. Brown (col. 2 lines, 34-40) teaches the function of an authority-enabled system:

"In accordance with the present invention, multiple authority-designated settings are accessed at an authority-enabled system via a network from a universally accessible database according to a particular universal identifier associated with a particular user. The particular user is only allowed access to a selection of multiple of types of content from the authority-enabled system that are enabled according to the authority-designated settings received at the authority-enabled system, such that an

authority-enabled system enforces an authority-designated access policy for a particular user received via a universally accessible database.".

It may appear that the function of M. Brown's authority-enabled system is similar to that of the authentication handler described in Claim 1. However, they are not the same. First, M. Brown does not have any description regarding how the user is authenticated. The role of the authority-enabled system is to enforce the access policy according to predefined authority-designed settings residing at a remote server system. In contrast, the role of the authentication handler does not enforce an access policy. Its main role is to verify a user's identity by communicating with the authentication gateway using Web services. Therefore, the function of the authority-enabled system is not the same as that of the authentication handler.

Second, M. Brown does not make any suggestion of using Web services as the communication method between the authority-enabled system and the remote server system. In contrast, Claim 1 describes that Web services is the key technology for the authentication handler to communicate with the gateway authority. Thus, Web services technology is foreign not only to Yu, Vaeth, but also to M Brown. Furthermore, the use of Web services makes the implementation of the authentication handler very easy. As a result, more web site owners are likely to implement the authentication handler and subscribe to a global authentication authority system for stronger authentication of their online users. Meanwhile, as more web sites are embracing this global authentication authority system, more online users will be attracted to use this system because of the convenience of only having to carry a single client authentication device to generate the one-time identity codes for access to a plurality of web sites. Thus, it is obvious that this global authentication authority system is far more superior to that of the local authentication system as described by Yu. This superiority of the global design will produce unexpected results.

Based on the above mentioned reasons, it is the applicants' opinion that the combination of Yu, Vaeth and M. Brown can not produce a system that meets the specifications as described in Claim 1. Thus, Claim 1 is unobvious and patentable over the referenced prior-art.

2) The method and system described in Claim 1 can produce Synergism.

The idea of using a local authentication server, authentication client, and one-time identity or password codes to authenticate a user to a system is already proven. However, the idea of developing a global authentication authority system which comprises four distinctive components (i.e., authentication authority, authentication handler, authentication gateway, and authentication client), and use Web services to connect them is new. This novel invention can produce a synergy effect. For example, under this system, a user is able to be identified as a "single" authentication client with the capability to log into a plurality of Internet web sites subscribing to the verification services from the authentication authority. This is a very important feature for consumers to embrace because of the convenience, and flexibility to authenticate with plural Internet web sites using one-time identity codes available from a single verification service.

Furthermore, the use of this system as described in Claim 1 can also be used to verify an individual's identity. Assume a consumer would like to buy a computer from ABC Inc. making the purchase over the phone. The current practice is to verbally supply the consumer's credit card information to ABC for purchase. Since ABC does not have a strong way to validate the consumer's identity, ABC is unable to more conclusively determine as to whether fraudulent use of the user's credit card has occurred. However, if an authentication system disclosed in this invention is implemented, the consumer may generate the additional verification information over the phone

using his/her authentication device to generate a one-time identity code and provide it to ABC. ABC then feeds the one-time identity code into its authentication handler for identity verification. Thus, this additional procedure greatly improves the security of conducting impersonal phone or Internet consumer transactions using credit card information.

There are numerous applications that can be derived from this novel invention as described in Claim 1 that are not only Internet or phone related transactions. For instance, the authentication client can be developed to be part of a credit/debit card payment system for everyday impersonal transactions such as self-serve gas pumps at an automobile fueling station, self-serve grocery check out counters, and banking ATM machines. Furthermore, the same authentication client device can also be developed to start an automobile or unlock doors with security keypads for house entry, since the authentication client device itself represents an identity factor that the user has in possession and generates a verifiable identity code. Many other security related applications can also be developed based on this global authentication authority invention. Therefore, the implication of synergism is obvious.

3) The system described in Claim 1 has not been implemented by the industry in the current market place.

Vendors are just beginning to develop and market stronger identity safeguard products for the consumer Internet online business. For example, the hardware token market leader RSA still employs its traditional business model for the consumer market, i.e., sell one-time identity tokens and authentication servers to reside at the Internet online business provider such as Etrade or AOL. The consumer must have a separate one-time identity hardware token for each service: one for Etrade, and another for AOL. As a result, a consumer may carry a plurality of tokens to access a plurality of Internet online services.

There is no vendor in the current market place that has a system available as described in Claim 1. This lack of presence from current vendors in the marketplace to offer a system as described in Claim 1 is also evidence of unobviousness.

4) The proto-typed system described in Claim 1 has been developed and tested by applicants for commercial use. The invented authentication authority web services are available over the Internet at www.globalkey.biz.

Claim 6

Claim 6 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to Vaeth. The use of Web services technology can produce unexpected results for the same reason as explained in the remark of Claim 1 above. Furthermore, the remark of Claim 1 also discusses the evidence of unobviousness for separating the gateway authority from the authentication authority.

Claim 8

Claim 8 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to Yu. The use of Web services technology for the authentication authority to independently generate one-time identity codes by communicating with the authentication client can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

Claim 9

Claim 9 is canceled.

Claim 10

Claim 10 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to Vaeth. The use of Web services technology for the authentication authority to communicate with the authentication handler can

produce unexpected results for the same reason as explained in the remark of Claim 1 above.

Claim 11

Claim 11 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to Yu. The use of Web services technology for the authentication client to synchronize with the authentication authority can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

Claim 14

The confirmation codes described in Claim 14 are used to verify the success of synchronization. In contrast, Yu's confirmation processes noted by last O.A. (p.8) are used to confirm a person's identity or to confirm a password for the legal use of the IC card by the owner, i.e., from Yu's (col. 6 lines 6-12) teaching:

"The user authentication system includes an IC card 100 for safely keeping and carrying personal secret information, a transaction terminal 120 which is miniature and portable for generating a one-time password to confirm the identity of a person and refer to an account balance of an electronic money, ...",

and from Yu's (col. 11 lines 50-56) other teaching

"If the process for confirming the password remembered by only the user is added to the user authentication process of the user authentication system according to the principles of the present invention, a safer user authentication is available. Namely, the user should own the password remembered by only the user, the IC card owned by only the user, ...".

Thus, Claim 14 describes a novelty concept which is foreign to Yu. The confirmation code of Claim 14 is for the success of the synchronization, while that of Yu's is to confirm a user's identity. It is obvious that Claim 14 solves a different problem than that of Yu. This demonstrates that Claim 14 is unobvious.

Claim 15

The non-predictable sequence number described in Claim 15 is a random number in nature. However, this random number is different from that described in Yu. Yu (col. 6, line15-16) teaches:

"The IC card 100 stores a secret key and a predetermined random number for generating a one-time password. ...".

And Yu (col. 7, line 13-17) also teaches:

"The first random number changer 124 changes the random number stored in the random number memory 122 into a predetermined value and stores the changed random number in the random number memory 122 after the one-time password is generated by the first password generator 123.".

Thus, the random number described in Yu is a predetermined random number and is stored by the random number changer. If there is a system breach, this stored predetermined random number can become a public knowledge. In contrast, the random number (non-predictable sequence number) described in Claim 15 is generated independently by the authentication authority and authentication client, respectively. It is secure and highly unpredictable. This arrangement can produce unexpected results and thus suggests that Claim 15 is not obvious.

Claim 18

Claim 18 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to Yu. The use of Web services technology for

the authentication client to communicate with the authentication authority can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

Claim 19

Claim 19 further adds "which support the use of Web services technology" for clarity. Web services technology is foreign to M. Brown. The use of Web services technology for the authentication handler to communicate with the authentication gateway can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

Claim 20

Claim 20 further adds "comprising the use of Web services technology" for clarity. Web services technology is foreign to M. Brown. The use of Web services technology can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

The last O.A. also notes (p. 10) that M. Brown (col. 6, lines 57-63) teaches:

"Accountability application 98 compares the product requested for purchase by the user with the authority-designed products and services and controls an access signal to check-point device 134 indicating whether or not the user is allowed access to purchase the particular book according to the authority-designed settings.".

The above M. Brown's teaching shows us that the main objective of M. Brown's invention is to provide a system which implements user access control in a granular level. In contrast, the function of the authentication handler as described in Claim 20 is to provide authentication control to verify a user's identity. Therefore, Claim 20 solves a different problem than the referenced M. Brown's art, and Claim 20 is unobvious.

The Rejection of Claims 2, 3, 4 and 5 Under 35 USC 103 (a) Overcome

The last O.A. rejected Claims 2, 3, 4 and 5 for being unpatentable over Yu et al (US Patent No. 6,067,621), Vaeth et al (US Patent No. 6,035,402), and Brown et al (US Patent No. 6,658,415, M. Brown), Brown et al (US Pub No, 2004/0199636 L. Brown).

Claim 2

The last O.A.notes (p.10) that L. Brown (paragraph 0025) teaches:

"Service providers 11 host a network accessible software module. A service provider defines a services description for a Web service and publishes it to a service registry 13, ..".

L. Brown teaches Web services fundamentals, Claim 2 does not claim the invention of Web services. Rather, Claim 2 addresses the use of Web services to provide authentication authority services. The use of Web services in the applicants' system can produce unexpected and synergetic results, because the use of Web services technology can lead to an easy integration of the authentication authority service. This will further lead to the prevalent adoption and use of the authentication authority system.

Although the last O.A. notes (p.10) that the combination of Yu, Vaeth, M. Brown, and L. Brown would have been obvious, it is inherent that by combining a large number (over three) references of prior art is evidence of unobviousness. Furthermore, as having stated before, the combination of Yu, Vaeth and M. Brown would produce an inoperative system. A significant modification of Vaeth's teaching is necessary. Thus, applicants' system is unobvious.

Claim 3

The last O.A. notes (p.11) that L. Brown's teaching describes Web services fundamentals. It describes the nature of WSDL and UDDI. Claim 3 also does not claim the invention of WSDL and UDDI. Rather Claim 3 addresses the use of WSDL and UDDI in the applicants' authentication authority system. The use of WSDL and UDDI in the applicants' system can produce unexpected and synergetic results.

Claim 4

The last O.A notes (p.12) about L. Brown's teaching is regarding the use of SOAP security extension, SSL and HTTP in IBM WebSphere Application Server 4.0. Claim 4 does not claim the invention of SOAP, SSL and HTTP. Rather Claim 4 addresses the use of SOAP, SSL and HTTP in the applicants' authentication authority system. The use of SOAP, SSL and HTTP in the applicants' system can produce unexpected and synergetic results, because the adoption of industry standard can produce a coherent system which is compatible with systems developed by other vendors. As a result, the applicants' authentication authority system can become a widely employed system in the market place.

Claim 5

The last O.A. notes (p.12) about L. Brown's teaching is regarding the transport of SOAP using IBM MQSeries, FTP, and mail messages. Claim 5 does not claim the invention of FTP or SMTP. Claim 5 addresses the use of FTP or SMTP to transport data in the applicants' authentication authority system. The use of FTP, SMTP in the applicants' system can produce unexpected and synergetic results, because FTP and SMTP can deliver the authentication authority service to more users.

The Rejection of Claims 7, 12, 13, 16 and 17 Under 35 USC 103 (a) Overcome

The last O.A. rejected Claims 7, 12, 13, 16 and 17 for being unpatentable over Yu et al (US Patent No. 6,067,621), Vaeth et al (US Patent No. 6,035,402), and Brown et al (US Patent No. 6,658,415, M. Brown), Vandergeest et al (US Pub No, 2002/0169988).

Claim 7

Claim 7 has been amended to add "comprising the use of Web services technology" for clarity. Web services technology is foreign to Vandergeest. The use of Web services technology can produce unexpected results for the same reason as explained in the remark of Claim 1 above.

The last O.A.also notes (p.13) that

"However Vandergeest teaches that authentication authority registers and manages user identity, authentication client identity (i.e. device ID), user private identity (i.e. password), and associated vital information (i.e. biometric information)".

It may appear that Vandergeest system contains an authentication authority. However, from Vandergeest's teaching (paragraph 0015), i.e.,

"Briefly, a method and apparatus provides user authentication by communicating primary authentication information, such as user identification data and/or password data to an authentication unit via a primary channel such as over the Internet. An authentication code is first generated by the authentication unit on a per session basis and is sent to the first device via an alternate or secondary channel during the session. The

authentication unit determines which intermediate destination unit will receive the generated authentication code.",

applicants realize that the concept of authentication authority is foreign to Vandergeest. Vandergeest describes an authentication unit system that operates as an alternate channel to the authentication client user. This authentication unit system is a local system. In contrast, the authentication authority system described in the applicants' invention is a global system which provides identification verification services for global users.

The last O.A. also notes (p.14) that

"it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Vandergeest into the teaching of Yu, Vaeth and M. Brown to use authentication unit and authentication database for registering and managing the user's multi-factor authentication information. The modification would be obvious because one of ordinary skill in the art would be motivated to utilize multi-factor authentication techniques for improving the authentication process as compare to two factor authentication."

It is the applicants' opinion that the combination of Yu, Vaeth, M. Brown, and Vandergeest would produce an inoperative system. To produce an operative system, a major modification of Vaeth's teaching is necessary. In addition, this system must combine the teaching of L. Brown for the concept of Web services. This means that five references (Yu, Vaeth, M. Brown, L. Brown, and Vandergeest) must be combined. The need to combine multiple references is evidence of unobviousness for the applicants' invention.

Claim 12

The last O.A. notes (p.14) that it would be obvious to combine the teaching of Yu and Vandergeest as the basis to reject Claim 12.

Applicants agree that Yu does not teach user identity, authentication client identity and user private identity as the input information. Applicants also agree that Vandergeest's system recognizes these identities as the input information. However, applicants realize that Vandergeest does not combine these identities to generate authentication codes. Instead, Vandergeest utilizes these identities as the input information for the authentication unit to send back authentication codes, because Vandergeest teaches (paragraph 0016):

"**Accordingly, in one embodiment, an authentication database is maintained which contains per-user destination unit data, including, for example, a destination unit identifier such as a phone number of a radiotelephone, an IP address, a pager number, or any other suitable intermediate destination unit identifier which the authentication unit can use to contact and send the authentication code.**".

In contrast, Claim 12 combines the user identity, authentication client (device) identity and user private identity to generate synchronization codes. Synchronization is not a process included in the Vandergeest system. Thus, the referenced arts (Yu and Vandergeest) do not contain any suggestion that they can be combined to meet Claim 12. This is an unsuggested combination.

Claim 13

Claim 13 is canceled.

Claim 16

The non-predictable sequence number described in Claim 15 is a random number which will be used for producing one-time identity codes. From Vandergeest's teaching (paragraph 0018), i.e.,

"The secondary authentication information is typically an authentication code generated on a per session basis. This may include, for example, a pseudo random number or other suitable information. The authentication unit searches the database based on, for example, the sent user ID, to determine the telephone number of a radiotelephone or pager number associated with the user requesting authentication. The authentication code is sent to the designated unit via a wireless back channel during the session. The authenticator then determines whether the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel to the third device.",

Vandergeest suggests that the random number is used as the authentication code. However, Vandergeest does not suggest employing the user identity, authentication client identity or private identity as the input information to generate the random number. Thus, the referenced arts (Yu and Vandergeest) do not contain any suggestion that they can be combined to meet Claim 16. This is an unsuggested combination.

Claim 17

According to Vandergeest's teaching (paragraph 0020), i.e.,

"During this session, the first unit 10 responds by sending the primary authentication information 32, namely, the user ID and password (if required). This may be provided, for example, by a person through an input device, such as a keypad. It may be a biometric input device, may be a hardware token, smart card or other suitable mechanism.",

the biometric data is sent from the first unit as the primary authentication information. In contrast, the biometric identity described in Claim 17 is not transported from the authentication client to authentication authority, and is only

used to compute a synchronization code and a non-predictable sequence number. This arrangement of the applicants' invention is to produce a non-predictable number for stronger security and extremely minimize if not make impossible the reproduction of this non-predictable number. In addition, the applicants' invention incorporates a high security consideration to prevent any client authentication or (i.e.) private identity information to be transported over the wire or over the air. Thus, the applicants' invention utilizes a new principle of operation with a higher security feature. The inclusion of a high security feature is a superior design and can produce unexpected results.

CONCLUSION

For all the above reasons, applicants submit that the claims are now in proper form, and that the claims all define patentable over the prior art. Therefore, they submit that this application is now in condition for allowance, which action they respectfully solicit.

Conditional Request for Constructive Assistance

Applicants have amended the claims of this application so that they are proper, definite, and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicants respectfully request the constructive assistance and suggestions in order that this application can be placed in allowable condition as soon as possible and without the need for further proceedings.

Chaing Chen
8778 Boulder Ridge RD
Laurel, MD 20723-5901
Tel. (301) 617-4370